AMENDMENTS TO THE CLAIMS

LISTING OF CLAIMS

The following listing of claims replaces all prior versions:

1-10. (Cancelled)

11. (Currently Amended) ~~The method of Claim 10 further comprising the step of:~~

A method of processing a digital signal comprising:

generating a local key at a host processor;

~~f) before transferring said local encryption key across said communication link,~~ encrypting said local ~~encryption~~ key at said host processor;

transferring said encrypted local key across a communication link from said host processor to a first integrated circuit and to a second integrated circuit;

encrypting said digital signal at said first integrated circuit using a decrypted version of said encrypted local key;

transferring said encrypted digital signal to said second logical circuit; and

decrypting said encrypted digital signal at said second logical circuit using a decrypted version of said encrypted local key.

12. (Currently Amended) The method of Claim 11 wherein said encrypting said local key ~~step f)~~ comprises ~~the steps of~~:

[[f1)]] said host processor accessing a value in a register in said first integrated ~~logical~~ circuit; and

[[f2)]] based upon said value accessed from said register ~~in said step f1),~~ encrypting said local ~~encryption~~ key.

13. (Currently Amended) The method of Claim 11 wherein said encrypting said local key ~~step f)~~ comprises ~~the steps of~~:

[[f1)]] said host processor accessing a value stored in a register in said second integrated circuit; and

[[f2)]] based upon said value accessed from said register ~~in said step f1),~~ said host processor encrypting said local ~~encryption~~ key.

14. (Currently Amended) The method of Claim [[10]] 11 further comprising ~~the step of~~:

[[f)]] issuing a command to said first integrated ~~logical~~ circuit to modify a header in said digital signal to indicate that said digital signal is encrypted.

15. (Previously Presented) The method of Claim 14 wherein the command further indicates a type of encryption wherein said type is between even and odd.

16. (Currently Amended) The method of Claim [[10]] 11 further comprising ~~the step of~~:

[[f)]] switching said local ~~encryption~~ key between odd and even encryption.

17. (Currently Amended) The method of Claim [[10]] 11 further comprising ~~the steps of~~:

[[f)]] polling a first hidden register in said first integrated ~~logical~~ circuit;

[[g)]] determining whether the value in said hidden register has been modified; and

[[h)]] stopping said processing of said digital signal if said hidden register has been modified.

18. (Currently Amended) The method of Claim 17 further comprising ~~the step of~~:

[[i)]] sending a message to a broadcast provider if said ~~step j) determined that said~~ hidden register was modified.

19-25. (Cancelled)

26. (New) A device for processing a signal, comprising:

a first integrated circuit comprising a broadcast decryptor operable to decrypt a broadcast signal using a broadcast key and a local encryptor operable to locally encrypt said decrypted broadcast digital signal using a local key;

a second integrated circuit coupled to said first integrated circuit and comprising a local decryptor operable to decrypt said locally encrypted signal using said local key; and

a host processor coupled to said first and said second integrated circuits via a communication link and operable to encrypt said broadcast key and transfer said encrypted broadcast key to said first integrated circuit via said communication link, wherein said host processor is further operable to encrypt said local key and to transfer encrypted versions of said local key to said first and said second integrated circuits via said communication link.

27. (New) A device as recited in Claim 26, wherein said host processor is further operable to determine said broadcast key.

28. (New) A device as recited in Claim 27, wherein said device is operable to receive a smartcard and wherein said host processor determines said broadcast key by interfacing with said smartcard.

29. (New) A device as recited in Claim 26, wherein said first integrated circuit is further operable to decrypt said local key using a value stored in a register.

30. (New) A device as recited in Claim 29, wherein said register is hidden.

31. (New) A device as recited in Claim 26, wherein said broadcast decryptor comprises a hidden register operable to hold a value for decrypting said encrypted broadcast key.

32. (New) A device as recited in Claim 26, wherein said first integrated circuit further comprises a plurality of hidden registers and a control register operable to store a value to indicate which of said hidden registers is used for local encryption.

33. (New) A method of processing a digital signal comprising:

transferring first and second encrypted local keys from a host processor to respective first and second logical circuits;

transferring an encrypted broadcast key from said host processor to said first logical circuit;

decrypting an encrypted broadcast signal with a decrypted version of said broadcast key at said first logical circuit;

locally encrypting said decrypted broadcast signal at said first logical circuit using a decrypted version of said first encrypted local key;

transferring said locally encrypted broadcast signal to said second logical circuit; and

decrypting said locally encrypted broadcast signal at said second logical circuit using a decrypted version of said second encrypted local key.

34. (New) A method as recited in Claim 33, further comprising encrypting said broadcast key at said host processor.

35. (New) A method as recited in Claim 34, wherein said encrypting said broadcast key at said host processor comprises:

said host processor accessing a value in a hidden register on said first logical circuit; and

said host processor using said value to encrypt said broadcast key.

36. (New) A method as recited in Claim 35, further comprising said host processor modifying the value in said hidden register.

37. (New) A method as recited in Claim 35, further comprising:

said host processor selecting at least one of a plurality of hidden registers on said first logical circuit to be used to encrypt said broadcast key; and

said host processor indicating said selection to said first logical circuit.

38. (New) A method as recited in Claim 33, wherein said encrypting said broadcast key at said host processor comprises:

said host processor accessing a value stored in memory on said first logical circuit; and

said host processor using said value to encrypt said broadcast key.

39. (New) A method as recited in Claim 38 wherein said value is based on user-dependent data.

40. (New) A method as recited in Claim 33, wherein said encrypted broadcast signal is substantially compliant with a Motion Pictures Experts Group (MPEG) format.